Общество с ограниченной ответственностью
«Воксис» (ООО «Воскис»)
620026, г. Екатеринбург, ул. Розы Люксембург, дом 19, 4 этаж

Приложение № 3.

к приказу № М126-07-21 от 01.07.2021.

УТВЕРЖДАЮ

Директор ООО «Воксис»

_____ А.А. Мосунов

«01» июля 2021 г.

Стандарт
в области информационной безопасности
для поставщиков услуг ООО «Воксис»
(Редакция 2)

Екатеринбург

2021 г.

Содержание

1. Введение

В настоящее время в деятельности ООО «Воксис» (далее – Общество) отмечается тенденция и экономическая потребность на передачу выполнения отдельных собственных бизнес-функций на основании договорных отношений сторонним (внешним) организациям, специализирующимся на предоставлении соответствующих услуг - поставщикам услуг (подрядчиков).

Основными причинами и целями передачи выполнения бизнес-функций поставщикам услуг (целями аутсорсинга), как правило, являются:

- содействие оптимизации и повышению эффективности деятельности Общества;
- оптимизация затрат и повышение эффективности деятельности, в том числе связанных с выполнением непрофильных (вспомогательных) бизнес-функций Общества;
- привлечение внешних специалистов, обладающих необходимой квалификацией, компетенцией, знаниями и опытом работы в областях, которые являются вспомогательными или непрофильными для Общества;
- снижение зависимости от ресурсных ограничений, в первую очередь финансовых и кадровых, для выполнения вспомогательных или непрофильных бизнес-функций.

Одними из основных видов бизнес-функций, которые рассматриваются Обществом в качестве приоритетных для возможной передачи на аутсорсинг, являются:

- функции, связанные с применением информационных технологий, обслуживанием и администрированием средств вычислительной техники, серверного и телекоммуникационного оборудования, с разработкой программного обеспечения;
- функции, связанные с финансовой деятельностью, функционалом back-офиса, call-центра, организационным и административным обеспечением;
- функции, связанные с хранением и обработкой информации, в том числе на внешних центрах обработки данных и облачных сервисах (облачных службах);
- функции обеспечения информационной безопасности (ИБ) Общества;
- административно-хозяйственные функции.

Несмотря на то что привлечение поставщиков услуг для аутсорсинга призвано способствовать повышению эффективности реализации бизнес-функций при сокращении затрат на их реализацию, в большинстве случаев передача выполнения бизнес-функций приводит к появлению новых рисков в деятельности Общества, включая риски нарушения ИБ. Передача выполнения бизнес-функций на аутсорсинг не снимает обязанности и не переносит ответственности Общества, включая вопросы обеспечения ИБ, предусмотренные законодательством РФ, в том числе нормативно-правовыми актами РФ.

Основными факторами нового риска нарушения ИБ при аутсорсинге являются:

- возникновение зависимости процессов обеспечения ИБ от деятельности поставщика услуг;
- возникновение зависимости устойчивости (непрерывности) выполнения бизнес-функций Общества от возможных сбоев и отказа объектов информационной инфраструктуры поставщика услуг в результате реализации угроз ИБ;
- недостаточный уровень организации поставщиком услуг систем обеспечения ИБ;
- неверная оценка ресурсов, возможностей (кадровых, финансовых, технических) и потенциала поставщика услуг, необходимых для выполнения взятых на себя обязательств по обеспечению ИБ при реализации бизнес-функций Общества;
- наличие в соглашении об аутсорсинге положений, реализация которых приведет к возникновению ограничений в деятельности Общества;
- возникновение зависимости выполнения бизнес-функций Общества от эффективности деятельности поставщика услуг и добросовестности выполнения соглашения об уровне услуг (SLA).

Указанные факторы порождают риск нарушения ИБ, к которому относятся следующие риски:
- риск бесконтрольного несанкционированного доступа к защищаемой информации при реализации бизнес-функций лицами, не являющимися работниками Общества;
- риск несанкционированного осуществления действий и операций, имеющих финансовые последствия как для Общества, так для контрагентов Общества и их клиентов;
- риск потери контроля над реализацией и уровнем зрелости процессов обеспечения ИБ и как следствие - риск потери контроля над уровнем обеспечения ИБ и киберустойчивости;
- риск нарушения бесперебойности бизнес-функций;
- риск несоблюдения требований законодательства РФ в области обеспечения ИБ, в том числе в части обеспечения режимов защиты служебной тайны и персональных данных (ПДн).

Указанные риски нарушения ИБ могут реализоваться в виде инцидентов ИБ, имеющих значимые финансовые или репутационные последствия, например:
- прерывание Обществом предоставления услуг на неприемлемый период времени;
- несанкционированные действия и операции;
- несоблюдение требований законодательства РФ в области обработки информации ограниченного доступа, в том числе ПДн и информации, составляющей инсайдерскую информацию, коммерческую тайну и другие виды служебных тайн (далее - защищаемая информация).

В ряде случаев ущерб от реализации указанных рисков не может быть компенсирован поставщиком услуг в рамках заключенных договорных отношений.

В связи с этим при привлечении для аутсорсинга поставщиков услуг следует обеспечить реализацию механизмов управления и контроля риска нарушения ИБ, создающую основу для обеспечения соответствия уровня риска нарушения ИБ при передаче бизнес-функций на аутсорсинг уровню риска, принятому самостоятельно Обществом.

Для достижения цели управления и контроля риска нарушения ИБ при аутсорсинге настоящий Стандарт в области информационной безопасности для поставщиков услуг ООО «Воксис» (Редакция 1) (далее – Стандарт) устанавливает базовые требования к мерам по обеспечению ИБ для поставщиков услуг (подрядчиков).

Настоящий стандарт распространяется на подразделения Общества, передающие на постоянной (непрерывной) основе на длительный срок выполнение следующих бизнес-функций (процессов) сторонним (внешним) организациям - поставщикам услуг, в рамках которых возникает новый риск нарушения ИБ:

- при выполнении которых осуществляется обработка информации, защищаемой в соответствии с требованиями законодательства РФ, несанкционированный доступ к которой, раскрытие (распространение), несанкционированное (неавторизованное) изменение, уничтожение (потеря) и (или) хищение создают условия для возникновения убытков Общества, его контрагентов или их клиентов;
- ненадлежащее выполнение которых поставщиком услуг создает условия для реализации или реализует инциденты ИБ.

Целью стандарта является установление требований к управлению и контролю риска нарушения ИБ при аутсорсинге, выполнение которых создает основу для обеспечения соответствия уровня риска нарушения ИБ при передаче бизнес-функций на аутсорсинг уровню риска нарушения ИБ, принятому самостоятельно Обществом, а также основу для уменьшения такого риска.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах Общества, а также в соглашениях (контрактах, пакетах договорных документов) с поставщиками услуг.

Обязательность применения настоящего стандарта может быть установлена договорами и соглашениями, заключенными Обществом.

2. Термины и определения

Аутсорсинг - передача Обществом на основании договора на длительный срок сторонней (внешней) организации - поставщику услуг выполнения бизнес-функций Общества, которые являются необходимыми для ее деятельности и которые в обычных условиях (без привлечения поставщика услуг) осуществлялось бы Обществом самостоятельно.

Поставщик услуг - обслуживающая организация, специализирующаяся на предоставлении услуг, которой Общество передает выполнение своих бизнес-функций на аутсорсинг.

Услуга - деятельность поставщика услуг по выполнению бизнес-функций Общества, переданных на аутсорсинг.

Существенные функции - бизнес-функции Общества:

1) при выполнении которых осуществляется обработка защищаемой информации, несанкционированный доступ к которой, раскрытие (распространение), несанкционированное (неавторизованное) изменение, уничтожение (потеря) и (или) хищение создают условия для возникновения убытков Общества, его контрагентов или их клиентов (далее - обработка защищаемой информации);

2) невыполнение или ненадлежащее выполнение которых поставщиком услуг создают условия для реализации или реализуют инциденты ИБ, связанные:

- с нарушением непрерывности предоставления Обществом услуг (далее - нарушение непрерывности предоставления услуг);
- с утечкой защищаемой информации; с совершением операций, имеющих финансовые последствия;
- с несоблюдением Обществом требований к обеспечению ИБ, установленных законодательством РФ.

Аутсорсинг существенных функций – аутсорсинг бизнес-функций, которые отнесены к существенным.

Соглашение об уровне услуг (SLA, Service Level Agreement) - соглашение между Обществом и поставщиком услуг, описывающее определенные полномочия и услугу, а также целевые показатели уровня услуги, зоны ответственности сторон - Общества и поставщика услуг.

3. Обозначения и сокращения

РФ - Российская Федерация;
ИБ - информационная безопасность;
ИТ - информационные технологии;
ПДн - персональные данные;
СВТ - средства вычислительной техники;
СВР - степень возможности реализации риска нарушения ИБ;
СТП - степень тяжести последствий от реализации риска нарушения ИБ;
SLA - соглашение об уровне услуг (Service Level Agreement);
НСД - несанкционированный доступ.

4. Риск нарушения информационной безопасности при аутсорсинге существенных функций

4.1. Обществу при аутсорсинге существенных функций следует рассматривать следующие факторы нового риска нарушения ИБ:

- возникновение зависимости процессов обеспечения ИБ от деятельности поставщика услуг;
- возникновение зависимости устойчивости (непрерывности) выполнения бизнес-функций Общества от возможных сбоев и отказа объектов информационной инфраструктуры поставщика услуг в результате реализации угроз ИБ;
- ненадлежащий уровень организации поставщиком услуг систем обеспечения ИБ;
- неверная оценка ресурсов, возможностей (кадровых, финансовых, технических) и потенциала поставщика услуг, необходимых для выполнения взятых на себя обязательств по обеспечению ИБ при реализации бизнес-функций Общества;
- возникновение зависимости выполнения бизнес-функций Общества от эффективности деятельности поставщика услуг и добросовестности выполнения соглашения об уровне услуг (SLA);
- наличие в соглашении об аутсорсинге положений, реализация которых приведет к возникновению ограничений в деятельности Общества, которые в том числе могут быть связаны:
- с досрочным односторонним прекращением поставщиком услуг обеспечения дополнительного уровня ИБ при предоставлении услуг аутсорсинга;
- с ограничением возможности контроля деятельности поставщика услуг и получения необходимой информации для контроля риска нарушения ИБ;
- с недостаточным уровнем обеспечения ИБ и ненадлежащим управлением риском нарушения ИБ в случае недостаточной детализации в соглашении обязанностей поставщика услуг;
- с зависимостью реализации обеспечения ИБ от содержания и качества деятельности лиц, не являющихся работниками Общества;
- с расширением состава внутренних нарушителей безопасности информации, обладающих легально предоставленными правами логического и (или) физического доступа.

4.2. При аутсорсинге существенных функций факторы, указанные в пункте 4.1 настоящего стандарта, создают новый риск нарушения ИБ, который должен управляться и контролироваться Обществом.

Основные виды риска нарушения ИБ Общества, связанные с аутсорсингом существенных функций, и возможные последствия от его реализации приведены в таблице 1.

Таблица 1. Виды операционных рисков и возможные последствия для Общества от их реализации при аутсорсинге существенных функций.

Вид риска Общества	**Последствия для Общества от реализации риска**
Операционный	Несоблюдение требований законодательства РФ в

риск, связанный с несоблюдением требований законодательства РФ и соглашений с контрагентами (правовой риск)	области обработки защищаемой информации; несоблюдение законодательства РФ в области обеспечения защиты информации; несоблюдение законодательства РФ и соглашений с контрагентами Общества в обеспечении непрерывности предоставления услуг в результате реализации угроз ИБ; возникновение ограничений на способность Общества предоставить необходимую и достоверную информацию контрагентам Общества.
Операционный риск, связанный с потерей (невозможностью) контроля обеспечения ИБ поставщиком услуг	Политика обеспечения ИБ поставщика услуг может не совпадать с политикой обеспечения ИБ Общества, а деятельность поставщика услуг в части обеспечения ИБ может осуществляться с учетом собственных интересов; потеря Обществом контроля над уровнем риска нарушения ИБ и уровнем зрелости реализации поставщиком услуг процессов обеспечения ИБ; отсутствие возможности и необходимой компетенции у Общества обеспечить надлежащий контроль деятельности поставщика услуг в части обеспечения ИБ при аутсорсинге существенных функций
Операционный риск, связанный с возможностью прерывания деятельности Общества в результате реализации угроз ИБ	Нарушение непрерывности предоставления услуг в случае реализации сбоев и отказа в работе информационной инфраструктуры поставщика услуг или в работе информационной инфраструктуры Общества в результате деятельности поставщика услуг; нарушение непрерывности предоставления услуг в случае реализации сбоев и отказа в обслуживании технических средств и систем защиты информации в результате действий поставщика услуг; возникновение уязвимостей защиты информации в результате действий поставщика услуг
Операционный риск, связанный с реализацией инцидентов ИБ, имеющих последствия для Общества	Нарушение непрерывности предоставления услуг; утечка информации конфиденциального характера; хищение материальных носителей, содержащих объекты интеллектуальной собственности; совершение несанкционированных операций, имеющих финансовые последствия, в том числе лицами, не обладающими соответствующими правами
Операционный риск, связанный с возникновением зависимости от поставщика услуг	Отказ поставщика услуг от выполнения своих обязательств по обеспечению ИБ перед Обществом, в том числе предусмотренных соглашением об аутсорсинге существенных функций; возникновение неприемлемых финансовых затрат у Общества в случае отказа поставщика услуг от своих обязательств; утрата у работников Общества необходимых компетенций,

	знаний и навыков, необходимых для обеспечения ИБ при возврате выполнения существенных функций с использованием собственных ресурсов; невозможность обеспечить необходимый уровень ИБ при возврате выполнения бизнес-функций в течение периода времени, приемлемого для Общества; увеличение временных затрат на выполнение бизнес-функций, связанное с территориальной удаленностью поставщика услуг (при нахождении на большом расстоянии от Общества или в другом часовом поясе); снижение гибкости в обеспечении ИБ при выполнении бизнес-функций, связанное с выполнением поставщиком услуг только тех требований, которые установлены соглашением об аутсорсинге
Операционный риск, связанный со снижением качества услуг по обеспечению ИБ, предоставляемых поставщиком услуг	Снижение лояльности и удовлетворенности клиентов и контрагентов Общества

5. Основные требования к управлению риском нарушения информационной безопасности при аутсорсинге существенных функций

5.1. Настоящий стандарт определяет ряд основных требований, для цели управления риском нарушения ИБ и контроля над ним при аутсорсинге существенных функций.

Реализация указанных ниже основных требований с учетом дальнейших положений настоящего стандарта способствует применению взвешенного подхода к передаче Обществом выполнения бизнес-функций поставщикам услуг на основе оценке объема потенциального риска нарушения ИБ.

При определении основных требований к управлению риском нарушения ИБ в настоящем стандарте предполагается, что аутсорсинг существенных функций может оказать существенное влияние на деятельность и стабильность функционирования Общества.

5.2. Основное требование 1. В случае планирования передачи выполнения бизнес-функций поставщикам услуг на аутсорсинг Обществу следует установить политику в отношении аутсорсинга существенных функций (далее - политика аутсорсинга).

Политика аутсорсинга должна среди прочего однозначно определять:

- возможность аутсорсинга бизнес-функций, при выполнении которых осуществляется обработка защищаемой информации;

- возможность аутсорсинга бизнес-функций, невыполнение или ненадлежащее выполнение которых поставщиком услуг создает условия для реализации или реализует инциденты ИБ;

- возможность аутсорсинга только в случае соблюдения требований законодательства РФ в области обработки ПДн и информации, составляющей служебную тайну, в частности возможность аутсорсинга в случае надлежащего получения соглашения субъектов ПДн;

- возможность аутсорсинга только в случае соблюдения требований законодательства РФ в области защиты информации;

- возможность аутсорсинга только в случае реализации Обществом надлежащего управления риском нарушения ИБ и контроля над ним.

Политика аутсорсинга существенных функций должна быть принята - исполнительным органом Общества.

В отношении аутсорсинга существенных функций Общество должно реализовать процедуры внутреннего контроля соответствия принятой политики аутсорсинга.

5.3. Основное требование 2. Общество должно разработать, применять и обеспечить контроль программы аутсорсинга, предусматривающей вопросы управления риском нарушения ИБ (далее - программа аутсорсинга).

Программа аутсорсинга должна определять:

- состав и содержание мероприятий по управлению риском нарушения ИБ при аутсорсинге существенных функций;

- состав и содержание мероприятий по мониторингу и контролю деятельности поставщика услуг по обеспечению ИБ при аутсорсинге существенных функций;

- возможность привлечения поставщиком услуг субподрядчиков при оказании услуг аутсорсинга, а также требования к таким субподрядчикам.

5.4. Основное требование 3. Общество должно обеспечить выполнение своих обязательств перед контрагентами, а также возможность проведения эффективного контроля выполнения требований в области защиты информации.

Обществу необходимо реализовать:

- регламентацию и применение организационных мер и технических средств, реализующих контроль доступа работников поставщика услуг и иных лиц к защищаемой информации, а также информационным (автоматизированным) обрабатывающим ее системам;

- обязательное сохранение за Обществом функций управления предоставлением доступа к защищаемой информации, а при технической невозможности - контроль выполнения функций по управлению предоставлением доступа к защищаемой информации поставщиком услуг.

5.5. Основное требование 4. Обществу следует привлекать поставщиков услуг для аутсорсинга существенных функций только после принятия поставщиком услуг всех необходимых мер по обеспечению ИБ и заключения соглашения, определяющего детальные условия и разграничение ответственности по обеспечению ИБ.

Детализация условий по обеспечению ИБ в соглашении должна обеспечивать возможность проведения оперативных мероприятий по мониторингу и контролю со стороны Общества деятельности поставщика услуг в части обеспечения ИБ.

Детальные требования к содержанию соглашения об аутсорсинге существенных функций установлены в разделе 8 настоящего стандарта.

Примерный перечень вопросов, которые могут использоваться для оценки поставщика услуг в части обеспечения ИБ, приведен в Приложении 1.

Базовый набор мер по обеспечению ИБ поставщиком услуг, приведен в Приложении 2.

При заключении соглашения с поставщиками услуг на осуществление аутсорсинга существенных функций Обществу следует обеспечить наличие следующих условий по обеспечению ИБ:

- обязанность поставщика услуг обеспечить соблюдение требований к защите информации, установленных для Общества, в том числе требований, установленных в области защиты персональных данных;
- составление перечня защищаемой информации, передаваемой на обработку и (или) хранение поставщику услуг;
- разграничение ответственности между Обществом и поставщиком услуг в части обеспечения ИБ;
- наличие у поставщика услуг лицензий по оказываемым видам деятельности в соответствии с законодательством о лицензировании отдельных видов деятельности;
- сохранение права Общества на контроль выполнения Обществом самостоятельно или с привлечением внешнего аудитора, определяемого Обществом, условий соглашения в части выполнения обязанностей по обеспечению ИБ, соблюдение порядка и (или) процедуры выполнения указанного контроля;
- обязанность поставщиков услуг уведомлять Общество об инцидентах, связанных с обеспечением ИБ, соблюдение порядка и (или) процедуры выполнения указанного уведомления.

5.6. Основное требование 5. Общество при принятии решения об аутсорсинге существенных функций, при котором предполагается трансграничная передача защищаемой информации, следует убедиться в соблюдении требований:

- законодательства РФ, регулирующего вопросы трансграничной передачи персональных данных;
- законодательства РФ, устанавливающего обязанность обработки и хранения персональных данных на территории РФ;
- законодательства РФ, регулирующего вопросы лицензирования отдельных видов деятельности;
- законодательства РФ, регулирующего вопросы обеспечения безопасности критической информационной инфраструктуры.

6. Содержание задач и зона ответственности руководства Общества при аутсорсинге существенных функций

6.1. Деятельность руководства Общества является ключевым фактором обеспечения должного уровня управления и контроля в отношении риска нарушения ИБ при аутсорсинге существенных функций. Одним из основных аспектов является наличие полного осознания руководством Общества, что передача при аутсорсинге поставщику услуг выполнения бизнес-функций не переносит на поставщика услуг ответственность, обязанности по обеспечению ИБ и риски нарушения ИБ Обществом.

6.2. Основным содержанием задач руководства Общества при аутсорсинге, определенным в настоящем стандарте, является:

- установление политики и программы аутсорсинга существенных функций в соответствии с требованиями к их содержанию, определенными в настоящем стандарте, и реализация контроля за их выполнением;
- установление механизмов управления и контроля в отношении уровня риска нарушения ИБ в рамках заключения соглашений с поставщиком услуг;
- контроль над реализацией и выполнением деятельности по управлению риском нарушения ИБ;
- принятие решения о возможности аутсорсинга только на основании оценки риска нарушения ИБ;
- обеспечение наличия плана действий Общества в случае отказа поставщика услуг от выполнения своих обязательств, реализация которого позволит обеспечить необходимый уровень ИБ для продолжения выполнения бизнес-функций в течение периода времени, приемлемого для Общества (стратегия "выхода").

7. Требования к проведению оценки поставщика услуг при аутсорсинге существенных функций

7.1. Одним из основных элементов успешной реализации управления риском нарушения ИБ при аутсорсинге существенных функций является всесторонняя оценка потенциала поставщика услуг выполнить свои обязательства в соответствии с требованиями по управлению риском нарушения ИБ, применяемыми Обществом.

Оценку поставщика услуг рекомендуется проводить перед заключением с ним соглашения об аутсорсинге, а также на периодической (регулярной) основе.

7.2. Основными целями оценки поставщика услуг являются:

- оценка ресурсов, потенциала и возможностей поставщика услуг обеспечить необходимый уровень ИБ при выполнении своих обязательств в рамках заключенного соглашения;
- оценка опыта и репутации поставщика услуг;

- оценка показателей деятельности поставщика услуг на основе метрик СВР, принятых Обществом для контроля и мониторинга риска нарушения ИБ при аутсорсинге существенных функций;
- оценка возможностей поставщика услуг обеспечивать выполнение обязательств Общества перед контрагентами, как если бы бизнес-функции, переданные на аутсорсинг, выполнялись самостоятельно Обществом.

7.3. При оценке ресурсов, потенциала и возможностей поставщика услуг Обществу необходимо учитывать следующие показатели:
- финансовое состояние поставщика услуг, наличие финансовых ресурсов, необходимых и достаточных для обеспечения ИБ при предоставлении Обществу услуг аутсорсинга на протяжении всего срока действия соглашения;
- наличие в штате поставщика услуг персонала в необходимом количестве и с достаточной квалификацией;
- наличие у поставщика услуг системы обеспечения ИБ;
- реализация политики обеспечения доверия к персоналу, которая должна соответствовать политике обеспечения доверия к персоналу, применяемой в Обществе. В составе реализации такой политики необходимо рассматривать:
- определение, выполнение и регистрацию процедуры контроля деятельности работников, обладающих совокупностью полномочий, определяемых их ролями, позволяющими получить доступ к защищаемой информации Общества;
- определение, выполнение и регистрацию процедуры приема на работу, реализующие принцип "знать своего работника", включающие проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов, а также проверку в части профессиональных навыков и оценку профессиональной пригодности;
- получение письменного обязательства работников поставщика услуг о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов;
- включение обязанности персонала поставщика услуг по выполнению требований к обеспечению ИБ, обработке ПДн, обеспечению сохранности защищаемой информации в трудовые контракты (соглашения, договоры) и (или) должностные инструкции;
- наличие у поставщика услуг необходимых лицензий, предусмотренных законодательством о лицензировании отдельных видов деятельности;
- показатели, характеризующие политику аутсорсинга поставщика услуг в части обеспечения ИБ.

Для оценки политики поставщика услуг может быть рекомендован перечень вопросов, представленный в Приложении 1.

7.4. В составе метрик СВР, характеризующих деятельность поставщика услуг, могут использоваться следующие:
- оценка уровня защиты информации, реализованного поставщиком услуг в соответствии с требованием законодательства РФ;

- оценка уровня соблюдения требования к непрерывности предоставления финансовых услуг, реализованного поставщиком услуг;
- оценка потенциала Общества обеспечить контроль уровня обеспечения ИБ после заключения соглашения с поставщиком услуг;

- наличие у поставщика услуг необходимого технического и (или) технологического обеспечения.

7.5. Важным фактором при выборе поставщика услуг является оценка его репутации:

- наличие положительной деловой репутации в области выполнения аутсорсинга существенных функций для иных организаций;
- наличие опыта разработки, реализации и поддержки решений по аутсорсингу существенных функций;
- наличие известных инцидентов ИБ.

7.6. При оценке возможности поставщика услуг обеспечить выполнение обязательств Общества следует рассмотреть следующие показатели:

- соблюдение требований к обеспечению ИБ, установленных для Общества законодательством РФ по защите информации;
- возможность осуществления Обществом деятельности по мониторингу и контролю риска нарушения ИБ;
- возможность Общества получать информацию о результатах проведения внешних аудитов обеспечения ИБ и внешних аудитов обеспечения непрерывности деятельности.

7.7. Общество может выполнить оценку поставщика услуг следующими способами:

- самостоятельно работниками Общества;
- с привлечением аудиторской или консалтинговой организации (независимой от поставщика услуг), обладающей необходимым опытом и компетенцией для проведения оценки поставщика услуг.

7.8. В качестве основного фактора при оценке поставщика услуг Обществом следует рассматривать соблюдение законодательства РФ в области трансграничной передачи защищаемой информации в соответствии с положением пункта 5.6 настоящего стандарта.

7.9. В качестве дополнительного фактора при оценке поставщика услуг Обществу следует рассматривать:

- зависимость деятельности поставщика услуг от субподрядчиков;
- результаты взаимодействия поставщика услуг с субподрядчиками;
- наличие у поставщика услуг страхования рисков, связанных с эксплуатацией его информационной инфраструктуры.

7.10. Оценка поставщика услуг должна носить периодический характер и входить в состав мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций.

8. Требования к содержанию соглашений об аутсорсинге существенных функций

8.1. Заключение с поставщиком услуг соглашения (контракта, пакета договорных документов) об аутсорсинге является одним из основных элементов управления и контроля в отношении риска нарушения ИБ при аутсорсинге существенных функций.

8.2. Содержание соглашения об аутсорсинге должно создать правовые условия для возможности обеспечения Обществом:

- контроля и мониторинга уровня риска нарушения ИБ;
- выполнения своих обязательств перед контрагентами.

8.3. Содержание соглашения об аутсорсинге должно однозначно среди прочего определять:

- перечень существенных функций, связанных с обработкой защищаемой информации или обеспечением ИБ (реализацией процессов обеспечения ИБ), передаваемых на аутсорсинг поставщику услуг;
- обязанности и разделение зоны ответственности поставщика услуг и Общества в обеспечении ИБ при аутсорсинге существенных функций;
- требования к показателям качества деятельности поставщика услуг, определяемым на основе метрик управления риском нарушения ИБ Обществом в рамках процедур управления риском;
- требования к уровню и качеству предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления финансовых услуг (требования к SLA) и к инструментам по мониторингу этого уровня;
- требования к гарантиям поставщика услуг (в том числе финансовым) в случае наступления риска нарушения ИБ;
- требования к инфраструктуре оказания услуг, включая инфраструктуру обеспечения ИБ и обеспечения непрерывности выполнения бизнес-функций и их восстановления после инцидентов ИБ;
- обязанность поставщика услуг обеспечить возможность проведения Обществом или привлекаемой Обществом консалтинговой или аудиторской организацией контрольных мероприятий в рамках мониторинга риска нарушения ИБ;
- обязанность по обеспечению сторонами конфиденциальности информации;
- обязанность поставщика услуг проходить периодический аудит с целью подтверждения качества предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления услуг;
- обязанность поставщика услуг информировать Общество об инцидентах ИБ, включая НСД к защищаемой информации, в течение 3-х часов после выявления инцидента ИБ, а также о мерах, предпринятых для управления наступившими инцидентами;

- порядок разбора конфликтов в случае нарушения поставщиком услуг

условий оказания услуг, а также в случае несогласия поставщика услуг признавать факт реализации риска нарушения ИБ или инцидента ИБ;

- обязанность поставщика услуг информировать Общество обо всех факторах, связанных с возникновением риска нарушения ИБ при аутсорсинге существенных функций, включая тип событий и обстоятельства их реализации;
- обязанность поставщика услуг передавать всю необходимую информацию Обществу для выполнения своих обязательств перед контрагентами и уполномоченными органами исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области защиты информации;
- возможность пересмотра и изменения условий соглашения по инициативе Общества в следующих случаях:
- наличие у Общества необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения ИБ при аутсорсинге существенных функций;
- наличие у Общества необходимости принять соответствующие меры для выполнения своих обязательств перед контрагентами, а также перед уполномоченными органами исполнительной власти;
- возможность проведения регулярных (не реже одного раза в квартал) встреч/совещаний представителей Общества и поставщика услуг для обсуждения статуса выполнения соглашения об аутсорсинге в части вопросов обеспечения ИБ;
- рекомендуемые основания для отказа Общества от исполнения соглашения с поставщиком услуг в одностороннем внесудебном порядке в случае:
- смены владельцев (участников) поставщика услуг;
- изменения финансового состояния поставщика услуг, его потенциала, ресурсов и возможностей в отношении выполнения услуг аутсорсинга существенных функций;
- нарушения поставщиком услуг требований к уровню и качеству предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления услуг (требования к SLA);
- препятствия (отказа) со стороны поставщика услуг реализации мониторинга и контроля риска нарушения ИБ со стороны Общества или со стороны независимой аудиторской организации;
- возникновения риска нарушения ИБ, превышающего уровень, определенный Обществом в качестве приемлемого;
- возникновения инцидентов нарушения ИБ;
- минимальный срок выполнения условий расторжения соглашения об аутсорсинге существенных функций, необходимый Обществу для возобновления выполнения бизнес-функций собственными ресурсами или с привлечением иного поставщика услуг в случаях расторжения действующего соглашения;
- условия привлечения поставщиком услуг субподрядчиков, предусматривающие:

- право Общества сохранить способность мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций в случаях привлечения поставщиком услуг субподрядчиков;
- ограничения на передачу субподрядчику обработки защищаемой информации;
- ответственность поставщика услуг за все действия субподрядчика в части вопросов обеспечения ИБ, в том числе ответственность за соблюдение законодательства РФ;
- обязанность поставщика услуг обеспечить уведомление и получать предварительное согласование Общества при привлечении субподрядчиков для выполнения существенных функций Общества;
- обязанность поставщика услуг предоставить Общества документы (в том числе политики, стандарты), разработанные поставщиком услуг для обеспечения ИБ;
- обязанность поставщика услуг обеспечить соблюдение требований к защите информации, установленных для Общества, в том числе:
- в области защиты информации ограниченного доступа, включая защиту ПДн;
- в области безопасности критической информационной инфраструктуры;
- в области лицензирования отдельных видов деятельности;
- политику предоставления поставщику услуг доступа к защищаемой информации и инфраструктуре Общества;
- описание контактных данных лица, ответственного за реализацию соглашения об аутсорсинге со стороны поставщика услуг, а также процедур эскалации возможных конфликтов при оказании услуг аутсорсинга;
- требования к работникам поставщика услуг, задействованным в обеспечении ИБ.

8.4. Целесообразно указать услуги (сервисы), которые будут поддерживаться поставщиком услуг в случае возникновения инцидентов ИБ.

8.5. При составлении соглашения об аутсорсинге необходимо привлекать представителей подразделения безопасности, операционных подразделений, юридической службы, а также подразделений информатизации Общества.

9. Хранение и архивирование

Подлинник настоящего Стандарта во время срока действия хранится в соответствии с требованиями Инструкции по делопроизводству в ООО «Воксис».

10. Рассылка и актуализация

Периодическая проверка данного Стандарта проводится сотрудником подразделения безопасности Общества по мере необходимости, но не реже 1 раза в 12 месяцев.

Решение об инициации процесса внесения изменений в Стандарт

принимает Директор по безопасности на основании предложений других подразделений, результатов применения документа в Обществе, анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних аудитов.

Приложение 1

Перечень вопросов для оценки политики поставщика услуг в части обеспечения информационной безопасности

1. Вопросы организации защиты данных

- Как данные Общества, включая защищаемую информацию, отделены от данных других клиентов?
- Где хранятся данные Общества, включая защищаемую информацию?
- Как обеспечивается конфиденциальность и целостность данных Общества, включая защищаемую информацию?
- Как осуществляется контроль доступа к данным Общества, включая защищаемую информацию?
- Как защищаются данные Общества в процессе их передачи поставщику услуг?
- Как защищаются данные Общества в процессе их передачи между различными подразделениями поставщика услуг, в том числе в процессе их передачи между различными центрами обработки данных, включая облачные?
- Как защищаются данные Общества в процессе их передачи субподрядчикам поставщика услуг?
- Реализованы ли меры по контролю утечек данных Общества?
- Может ли третья сторона, в том числе правоохранительные органы, операторы связи, хостинг-провайдеры, получить доступ к данным Общества? Какие правила и механизмы доступа должны применяться?
- Все ли данные Общества уничтожаются по завершении договора на оказание услуг аутсорсинга?

2. Вопросы анализа защищенности

- Как часто проводится анализ защищенности сети и приложений поставщика услуг и его субподрядчиков?
- Может ли Общество провести собственный анализ защищенности поставщика услуг аутсорсинга? Какова процедура проведения анализа защищенности?
- Каков процесс устранения обнаруженных уязвимостей?
- Существуют ли результаты анализа защищенности инфраструктуры поставщика услуг со стороны третьих фирм?

3. Вопросы управления доступом

- Возможна ли интеграция с каталогом учетных записей Общества?
- Как осуществляется управление учетными записями в информационных

системах поставщика услуг?

- Поддерживается ли Single Sign-On (SSO)? Какой стандарт применяется для реализации SSO?

4. Вопросы охраны и персонала

- В каком режиме обеспечивается контроль доступа на территорию поставщика услуг и его субподрядчиков (8x5 или 24x7)?
- Поставщик услуг и его субподрядчики пользуются выделенной инфраструктурой, включая помещения, или разделяют ее с другими организациями?
- Регистрируется ли доступ персонала поставщика услуг и субподрядчиков к данным, включая защищаемую информацию, Общества?
- Какова процедура набора персонала поставщиком услуг и его субподрядчиками?

5. Вопросы доступности и производительности

- Каков обеспечиваемый поставщиком услуг и его субподрядчиками уровень качества обслуживания (SLA)?
- Какие меры обеспечения доступности используются поставщиком услуг и его субподрядчиками (например, резервные каналы связи, защита от DDoS)?
- Какие инструменты контроля доступности инфраструктуры поставщика услуг предоставляются Общества?
- Существует ли у поставщика услуг план действий на время нарушения доступности инфраструктуры?

6. Вопросы безопасности приложений

- Существует ли у поставщика услуг процесс тестирования внешних приложений и исходного кода?
- Использует ли поставщик услуг или его субподрядчики приложения третьих фирм при оказании услуг аутсорсинга?
- Каковы используемые меры защиты приложений (например, WAF, защита БД)
- Внедрен ли поставщиком услуг и его субподрядчиками процесс безопасного программирования (SDLC) при разработке приложений?

7. Вопросы управления инцидентами

- Согласовано ли понятие инцидента ИБ и их перечень между Обществом и поставщиком услуг?
- Существует ли у поставщика услуг и его субподрядчиков план реагирования на инциденты?
- Каков процесс реагирования на инциденты?

8. Вопросы обеспечения сохранности защищаемой информации

- Какие данные собираются поставщиком услуг или его субподрядчиками об Общества? Где и как долго они хранятся?
- Каковы условия передачи данных Общества третьим лицам?
- Каковы гарантии поставщика услуг относительно нераскрытия защищаемой информации Общества третьим лицам и третьими лицами?
- Существует ли у поставщика услуг процесс обезличивания защищаемой информации и предоставления к ней доступа только авторизованному персоналу?

9. Вопросы обеспечения непрерывности бизнеса и восстановления после инцидентов ИБ

- Существует ли у поставщика услуг и его субподрядчиков план обеспечения непрерывности бизнеса и восстановления после катастроф?
- Существует ли у поставщика услуг и его субподрядчиков резервная инфраструктура, включая центр обработки данных?
- Проходил ли поставщик услуг внешний аудит по непрерывности бизнеса и восстановлению после катастроф?

10. Вопросы регистрации событий безопасности

- Как поставщиком услуг и его субподрядчиками обеспечивается регистрация событий безопасности и сбор доказательств по инцидентам ИБ?
- Как долго хранятся журналы регистрации событий? Какова периодичность ротации журналов регистрации? Возможно ли увеличение этого срока?
- Можно ли организовать хранение журналов регистрации событий во внешнем хранилище?

11. Вопросы соответствия требованиям

- Подчиняется ли поставщик услуг или его субподрядчики локальным, национальным или международным нормативным требованиям? Каким?
- Проходил ли поставщик услуг или его субподрядчики внешний аудит на требования обеспечения ИБ?
- Проводит ли поставщик услуг регулярную оценку рисков нарушения выполнения требований заказчиков, в том числе Общества?
- Внедрены ли средства контроля, обеспечивающие полное, точное и своевременное оказание услуг, снижающие выявленные риски?

12. Вопросы финансовых гарантий

- Существует ли компенсация в случае инцидента безопасности или нарушения соглашения о качестве обслуживания (SLA)?

13. Вопросы завершения договорных обязательств

- Какова процедура завершения договорных обязательств?
- Как осуществляется возврат защищаемой информации и в каком виде (формате)?
- В течение какого срока по окончании договорных обязательств поставщик услуг возвратит все данные Общества?
- Каков процесс уничтожения всех резервных и иных копий данных Общества?

14. Вопросы интеллектуальной собственности

- Кому принадлежат права на данные, переданные Обществом поставщику услуг? Кому принадлежат права на данные, полученные в процессе оказания услуг аутсорсинга Общества поставщиком услуг (в том числе журналы регистрации, резервные копии, репликации БД, базы инцидентов)?

Приложение 2

Базовый набор мер по обеспечению информационной безопасности поставщиком услуг.

Общие меры по обеспечению информационной безопасности	**Как реализовано**
Для выполнения операций по обеспечению безопасности должны быть назначены ответственные лица.	
Использование мобильных телефонов, планшетов (в том числе для зарядки аккумуляторных батарей от рабочей станции), видео-, звукозаписывающей аппаратуры работниками в обязанности которых входит обслуживание входящих и исходящих вызовов, прослушкой диалогов, в операторских залах (а также в залах, предназначенных для обучения) запрещается.	
Для каждой учетной записи информационной системы должен быть определен сотрудник или группа сотрудников, несущих ответственность за ее использование	
Каждый работник поставщика услуг (подрядчика) должен использовать предоставленные доступы в информационные системы только для выполнения служебных обязанностей	
При увольнении или переводе на иную работу системных администраторов поставщика услуг в течении 1 суток должны быть сменены все известные им пароли, в т.ч. от привелегированных учетных записей.	
В целях расследования инцидентов ИБ на рабочих местах должно быть включено журналирование (логирование) событий безопасности операционной системы.	
Безопасность рабочих мест	
Должно использоваться лицензионное, официально приобретенное программное обеспечение. Применение бесплатного или условно бесплатного программного обеспечения согласовывается с Обществом.	

Общие меры по обеспечению информационной безопасности	Как реализовано
Должно быть запрещено (и заблокировано) использование личной электронной почты (и иных средств коммуникации – мессенджеры).	
На рабочих станциях и серверах должны быть задействованы механизмы автоматической блокировки экрана после периода отсутствия активности более 15 минут, а также ручной блокировки, в случае оставления рабочего места без присмотра, для выхода из этого режима должен требоваться повторный ввод пароля.	
На рабочих станциях должна быть заблокирована возможность использования USB портов и съемных носителей информации.	
Права пользователя на рабочем месте должны быть максимально ограничены и не позволять осуществлять действия по изменению программно-аппаратного обеспечения, в т.ч. отключать средства защиты информации.	
Правами на изменения программно-аппаратного обеспечения, а также заведение новых пользователей и назначение им полномочий в системе должны быть наделены специально назначенные работники.	
Применяемое системное и прикладное программное обеспечение должно своевременно обновляться с использованием автоматизированных средств обновлений.	
Пароли / парольные фразы должны соответствовать следующим требованиям: минимальная длина не менее восьми символов, содержат цифры, заглавные буквы, строчные буквы и специальные символы.	
Пароль доступа в информационные системы должен выдаваться индивидуально и храниться пользователями в тайне. В случае утери или компрометации пароля должна создаваться заявка на его смену в течении 1 суток.	
Все системные пароли привилегированных учетных записей типа root, sa, Administrator должны меняться не реже 1 раза в квартал сотрудниками, отвечающими за работу с паролями и храниться на защищенном носителе информации или в запечатанном конверте в защищенном месте у руководителей тех подразделений, чьи администраторы используют данные пароли; Пароли специальных учетных записей, необходимых для функционирования различных	

Общие меры по обеспечению информационной безопасности	Как реализовано
системных сервисов, должны соответствовать требованиям, предъявляемым к привилегированным учетным записям администраторов, не должны тиражироваться, срок использования пароля не должен быть ограничен автоматически, тем не менее, администратор ИС должен производить регулярное его изменение;	
При работе с паролями запрещается: • сообщать свой пароль кому-либо, включая сотрудников Общества, администраторов, специалистов подразделений безопасности, руководителей и членов семьи; • требовать от других работников сообщить свой пароль; • использовать чужие пароли для входа в ИС; • использовать в качестве пароля слово из словаря (использование наборов русских или английских букв алфавита, в совокупности несущих смысловую нагрузку или значение в русском или английском языках), сленга, диалекта, персональную информацию (имена членов семьи, адреса, телефоны, даты рождения и т.п.); • использовать один и тот же пароль для регистрации в разных ИС Общества, если они не используют механизм «единого входа»; • хранить пароли для доступа на компьютерах и других средствах хранения информации (Flash-накопители, мобильные телефоны, планшеты и др.) в незашифрованном виде; • хранить пароли в доступной для чтения форме на бумаге, в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ; • осуществлять ввод пароля в присутствии посторонних лиц; • использовать индивидуальные пароли для коллективного доступа к ИС.	
Доступ к информационным ресурсам	
Доступ к информационным ресурсам предоставляется только штатным работникам на основании заявки.	
При увольнении работника должна в срок 24 часа должна формироваться заявка на блокировку учетной записи.	

VOXYS

Общество с ограниченной ответственностью
«Воксис» (ООО «Воксис»)
620026, г. Екатеринбург, ул. Розы Люксембург, дом 19, 4 этаж

Общие меры по обеспечению информационной безопасности	Как реализовано
Реагирование на инциденты информационной безопасности	
Должно быть организовано информирование Департамента безопасности Общества о всех случаях возникновения инцидентов информационной безопасности в срок 24 часа	
При возникновении инцидента информационной безопасности должны безотлагательно предприниматься все необходимые меры по предотвращению и минимизации ущерба и информированию Общества.	
Доступ в сеть Интернет	
Доступ в сеть общего пользования Интернет с рабочих мест должен предоставляться минимально необходимый для выполнения трудовых обязанностей по проекту.	
Использование Интернета для своих личных целей: посещение развлекательных, игровых, музыкальных, порнографических, террористических сайтов запрещено.	
Доступ к ресурсам Интернет должен осуществляться после авторизации пользователя на внутреннем сервере аутентификации (прокси-сервере, шлюзе доступа). Доступ в сеть Интернет должен журналироваться (логироваться), журналы (логи) должны храниться не менее 1 месяца.	
Антивирусная безопасность	
В целях непрерывного и комплексного обеспечения системой антивирусной безопасности все рабочие места и серверы должны быть оснащены лицензионным антивирусным программным обеспечением. За поддержание работоспособности антивирусного программного обеспечения и актуальности антивирусных баз отвечает IT-подразделение.	
Антивирус должен иметь систему централизованного обновления и управления. Антивирусные базы должны обновляться не реже 1 раза в сутки. Должна осуществляться регулярная проверка рабочих станций и серверов на наличие вредоносного ПО.	
Настройки антивирусной защиты должны обеспечивать выявление и предотвращение попадания в корпоративную сеть всех видов вредоносного ПО. При этом любое действие, выполненное с вредоносным ПО, должно регистрироваться в журнале событий антивирусного ПО.	

Общие меры по обеспечению информационной безопасности	Как реализовано
Настройки рабочего места пользователя не должны предоставлять пользователю возможность вмешательства в конфигурацию локального Агента антивирусной защиты.	
Электронная почта	
Сервис (услуга) корпоративной электронной почты предоставляется работникам исключительно для выполнения ими их должностных обязанностей.	
Сообщения электронной почты должны проходить следующие проверки: • на наличие вредоносного программного обеспечения; • на наличие спама; • на наличие файлов запрещённого типа; • на наличие вложений, не поддающихся анализу; • на наличие информации конфиденциального характера; • на наличие информации, содержащей коммерческую тайну; • на допустимый размер почтового сообщения.	
Использование публичных почтовых серверов для выполнения производственных задач допустимо в исключительных случаях по согласованию с Департаментом безопасности Общества.	
Для обмена информацией ограниченного доступа посредством электронной почты должны использоваться средства шифрования сообщений.	
При использовании электронной почты Общества запрещается: • создавать и распространять почтовые сообщения, содержащие сведения, направленные на возбуждение национальной, расовой или религиозной вражды, унижение национального достоинства, а равно пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, национальной или расовой принадлежности; • использовать провокационные или оскорбительные высказывания, касающиеся пола, национальной и расовой принадлежности, возраста, сексуальной ориентации, религиозных верований и практик, политических взглядов и происхождения; • создавать и распространять почтовые сообщения, содержащие материалы	

Общие меры по обеспечению информационной безопасности	Как реализовано
развлекательного характера; • осуществлять посредством КЭП пересылку материалов, нарушающих действующее законодательство РФ (вредоносное программное обеспечение, программное обеспечение для несанкционированного доступа, порнографию и т.д.); • использовать КЭП для непроизводственных целей; • открывать и запускать файлы, полученные от неизвестных адресатов, для которых невозможно определить принадлежность ни к одной из известных групп пользователей, как Общества, так и сторонних организаций (подобные файлы подлежат удалению); • посылать почтовые сообщения, содержащие исполняемые (com, exe, cmd, pif, bat, msi, jar и т.п.) файлы вложений; • запускать на пользовательских АРМ полученные по электронной почте исполняемые (com, exe, cmd, pif, bat, msi, jar и т.п.) файлы; • направлять внешним адресатам почтового сервера Общества почтовые сообщения, содержащие информацию, отнесенную к коммерческой тайне Общества, а также персональные данные; • создавать правила, автоматически переадресовывающие любые входящие почтовые сообщения на внешний почтовый ящик; • использовать свой адрес электронной почты Общества для оформления подписок, не относящихся к производственной деятельности; • публиковать свой адрес электронной почты Общества, либо адреса почты сотрудников Общества, на общедоступных Интернет ресурсах в непроизводственных целях; • при увольнении удалять сообщения электронной почты Общества до полной передачи дел другому работнику.	
Сетевая безопасность	
Подсистемы, АРМ, сервера поставщика услуг, используемые в интересах Общества, объединяются в выделенные сегменты с применением сертифицированных и согласованных с подразделением безопасности Общества средств, позволяющих реализовать дополнительные требования (межсетевые экраны, виртуальные сети, DMZ и т.п.).	

VOXYS

Общество с ограниченной ответственностью
«Воксис» (ООО «Воксис»)
620026, г. Екатеринбург, ул. Розы Люксембург, дом 19, 4 этаж

Общие меры по обеспечению информационной безопасности	**Как реализовано**
Доступ извне работников поставщика услуг к инфраструктуре Общества или обслуживаемого проекта может осуществляться только с использованием VPN-соединений и только при согласовании схемы доступа с Обществом.	
Инженерно-техническая безопасность	
На территории организации-субподрядчика должны быть внедрены системы контроля и управления доступом и видеонаблюдения с целью исключения нахождения на объекте посторонних лиц, расследования инцидентов.	
Должны быть разработаны и выполняться инструкция о пропускном и внутриобъектовом режимах и положение о видеонаблюдении.	
Персонал	
Все вновь принимаемые работники должны подписывать соглашение о конфиденциальности.	
Должна быть организована и проводится проверка документов, предоставляемых кандидатами при трудоустройстве в организацию поставщика услуг («скоринговые» проверки).	
Дополнительные требования к РМ операторов	
Фон рабочего стола должен быть обезличен. Не должно быть специфических для Партнера ярлыков на рабочем столе и в меню пуск, т.е. убрать все спец. ПО и ярлыки, которые не используются для обслуживания проекта	
Во время обслуживания звонков операторы Партнера не должны открывать свои внутренние сайты/программы, в которых будет идентифицироваться рабочее место	
Не должно быть видно наименование УЗ, под которой оператор вошел в ПК	

Общество с ограниченной ответственностью
«Воксис» (ООО «Воксис»)
620026, г. Екатеринбург, ул. Розы Люксембург, дом 19, 4 этаж

Общие меры по обеспечению информационной безопасности	Как реализовано
В раскладке клавиатуры нужно убрать все языки, кроме русского и английского	
При использовании браузера, в избранном не должно быть ресурсов, которые не требуются для проекта	
Язык системы и региональные настройки должны быть русскими или английскими	
Проверить нет ли подключенных сетевых папок, где видно доменное имя Партнера	